1. A method of detecting vulnerabilities in source code comprising:

   generating a model which describes certain characteristics about the flow of a routine, and

   using the model in conjunction with pre-specified criteria for the corresponding routine to determine whether the routine calls possess vulnerabilities as a consequence of the flow of the routine.

2. The method of claim 1 wherein the vulnerabilities are race conditions.

3. The method of claim 1 wherein the pre-specified criteria for the corresponding routine includes rules about the semantic behavior of the routine.

4. A system for detecting vulnerabilities in source code comprising:

   computer implemented logic for generating a model which describes certain characteristics about the flow of a routine, and

   computer implemented logic for using the model in conjunction with pre-specified criteria for the corresponding routine to determine whether the routine possesses vulnerabilities as a consequence of the flow of the routine.

5. The system of claim 4 wherein the computed implemented logic for using the model in conjunction with pre-specified criteria for the corresponding routine to determine whether the routine possesses vulnerabilities as a consequence of the flow of the routine includes a database specifying rules to detect vulnerabilities based on an analysis of the argument models.